UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,697	03/31/2000	Michael F. Angelo	COMP:0061	3660

7590 06/15/2005		EXAMINER

Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Ft. Collins, CO 80527-2400

	EXAMINER
	TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)
	09/540,697	ANGELO ET AL.
	Examiner	Art Unit
	Thanhnga B. Truong	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03/25/2005 (Amendment)</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-55</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-55</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>31 March 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04)   Office Action Summary   Part of Paper No./Mail Date 060305

DETAILED ACTION

1.   Applicant's amendment filed on March 25, 2005 has been entered. Claims 1-55 are pending. Claims 29 and 42 are amended by the applicant

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-10, 12-19, 21-30, 32-36, 38-43, 45-49, and 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (US 5,778, 070), and further in view of Miller (US 6,308,265 B1).

      a.   *Referring to claim 1:*

          i.   Mattison teaches:

(1)   a first section of non-volatile memory configured to store a BIOS program, the first section of non-volatile memory being reprogrammable **[i.e., the BIOS is stored in flash memory to allow for field updates and reprogramming of the BIOS (column 1, lines 56-57). In fact, referring to Figure 2, typically the upper 64 kilobytes in the first megabyte of the original PC architecture is allocated for BIOS (column 7, lines 21-23)]**; and

(2)   a second section of non-volatile memory operatively coupled to the first section of non-volatile memory, the second section of non-volatile memory being configured to store a boot-block program **[i.e., referring to Figure 2, "a boot-block program" is considered to also store in a flash memory 108 (column 5, line 55) and any extensions to the BIOS is contained in a region below the 64 kilobytes allocated to the BIOS, along with any other "program memory", in which a boot-block program is inherently provided (column 7, lines 23-25)]**;

(3)   the boot-block program having a first validation routine configured to validate the BIOS program stored in the first section of non-volatile

memory, and the BIOS program having a second validation routine configured to validate the boot-block program stored in the second section of non-volatile memory **[i.e., referring to Figure 3, in block 308, the current program in flash memory 108 is for verifying and/or validating the source and content of the flash memory upgrade program, whereby "a first validation routine configured to validate the BIOS program and a second validation routine configured to validate the boot-block program" are considered to include in this part of the upgrade program (column 9 lines 38-40)].**

      ii.   Although, Mattison does not explicitly mention the flash memory could store the boot block program, Miller teaches:

      (1)   Figure 3 is a flow chart describing the method according to the present invention. Such a method is applicable to a symmetrical flash part, in which boot block code (say of 16 Kbyte size) is stored in a first region of the flash part, and with a beginning portion (say the first 48 Kbytes) of updatable BIOS code also stored in the first region. For ease in explanation and not by way of limitation, the first region (segment) and all other regions (segments) of the symmetrical flash part have a size of 64 Kbytes. In the example, the remaining portion of the BIOS code is stored in a second region contiguous (in a memory addressable sense) with the first region **(column 5, lines 32-44; see also column 3, lines 31-51).**

      iii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

      (1)   clearly point out the boot block program resides within the flash memory for protecting the flash recovery code that formerly resides in a protected boot block segment of a non-symmetrical flash part **(column 3, lines 25-27 of Miller).**

      iv.   The ordinary skilled person would have been motivated to:

      (1)   clearly point out the boot block program resides within the flash memory for protecting boot block code while allowing an update to other code or data residing in the same block **(column 3, lines 29-31 of Miller).**

      b.   *Referring to claim 2:*

i.   Mattison further teaches:

(1)   wherein the first section of non-volatile memory comprises a protected segment of a reprogrammable memory device **[i.e., because the BIOS is the first program to gain control of the processor after reset, it is critical to any security scheme. Therefore, the BIOS must be protected from modification during any time where the machine is in an unsecured operating mode, especially in cases where the BIOS is stored in flash memory. The BIOS is stored in flash memory to allow for field updates and reprogramming of the BIOS (column 1, lines 50-57)]**.

c.   *Referring to claim 3:*

i.   Mattison further teaches:

(1)   wherein the second section of non-volatile memory comprises a reprogrammable segment of the reprogrammable memory device **[i.e., any extensions to the BIOS is contained in a region below the 64 kilobytes allocated to the BIOS, that is "the second section", along with any other "program memory" (column 7, lines 23-25)]**.

d.   *Referring to claim 4:*

i.   This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above

e.   *Referring to claim 5:*

i.   Mattison further teaches:

(1)   wherein the first section of non-volatile memory comprises a first memory device **[i.e., referring to Figure 2, "a first memory device " is considered to include in a flash memory 108]**.

f.   *Referring to claim 6:*

i.   Mattison further teaches:

(1)   wherein the second section of non-volatile memory comprises a second memory device **[i.e., referring to Figure 2, "a second memory device" is considered to include in a flash memory 108]**.

g.   *Referring to claims 7-10:*

i.   Mattison further teaches:

(1)   wherein the boot-block program comprises a public key and a hash algorithm used to validate the BIOS program; wherein one of the boot-block program and the BIOS program comprises an encrypted hash correlative to the BIOS program; wherein the encrypted hash is encrypted using a private key correlative to the public key; wherein the boot-block program validates the BIOS program by calculating a first hash of the BIOS program using the hash algorithm, using the public key to decrypt the encrypted hash to produce a second hash, and comparing the first hash to the second hash **[i.e., Figure 3 shows a series of operations for reprogramming flash memory 108. In block 302, a flash memory upgrade program containing a new flash memory image (e.g., a new BIOS image) for flash memory 108 (containing the current BIOS) would be loaded into system memory 106 and executed. The flash memory upgrade program would incorporate a digital signature which is "signed" by the private key of the vendor; the digital signature being the original hash value of the flash memory upgrade program after the original hash value has been encrypted with the vendor's private key. Operation would then continue with block 304. In block 304, after the flash memory upgrade program begins execution, the flash memory upgrade program would call a special function in the current program contained in flash memory 108, requesting to install the new flash memory image. This call would specify the address and size of the flash memory upgrade program located in system memory 106. Therefore, when the flash memory upgrade program (containing the new BIOS image) begins execution, it transfers control to the program contained in flash memory 108 (the current BIOS), requesting to update the current BIOS, that is "to validate the BIOS program" (column 7, lines 64-67 through column 8, lines 1-20)].**

h.   _Referring to claims 11-15:_

i.   Mattison further teaches:

(1)   wherein the boot-block program does not allow the system to boot if the first hash does not match the second hash, and wherein the boot

block program does allow the system to boot if the first hash matches the second hash; wherein the system warns a user if the first hash does not match the second hash; wherein the boot-block program allows the system to boot if the first hash does not match the second hash; wherein the boot-block program allows the system to boot if the first hash does not match the second hash in response to an instruction to boot from the user; wherein various system resources are enabled or disabled depending upon whether the first hash matches the second hash **[i.e.., In block 308, the current program in flash memory 108 would then verify the source and content of the flash memory upgrade program (which includes the new flash memory image) by: (a) decrypting the digital signature using the vendor's public key stored in the current program to obtain the original hash value; (b) independently calculating a hash value for the flash memory upgrade program which is resident in main system memory; and (c) comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match. If the hash values match, indicating that the flash memory upgrade program contained in main memory originated from the authorized creator AND has not been modified, then operation will continue with block 310. If the hash value does not match, the upgrade will be aborted. In an alternate embodiment, the user can be notified of the failed upgrade in another step (not shown), whereby the routine for allowing to boot up the system is inherently provided in the flash memory upgrade program (column 9, lines 38-58)].**

        i.   *Referring to claims 16-19:*

            i.   These claims have limitations that is similar to those of claims 7-10, thus they are rejected with the same rationale applied against claims 7-10 above.

        j.   *Referring to claims 20-24:*

            i.   These claims have limitations that is similar to those of claims 11-15, thus they are rejected with the same rationale applied against claims 11-15 above.

        k.   *Referring to claim 25:*

      i.   Mattison further teaches:

         (1)   CMOS memory operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory **[i.e., referring to Figure 2, "CMOS memory" is considered to include in system memory which couples to flash memory 108, that is "a non-volatile memory"]**; and

         (2)   non-volatile random access memory (NVRAM) operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory **[i.e., referring to Figure 2, "non-volatile random access memory (NVRAM) operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory at least one of the first section of non-volatile memory and the second section of non-volatile memory" is considered to include in flash memory 108]**.

     l.   *Referring to claims 26 and 27:*

      i.   Mattison further teaches:

         (1)   wherein the first validation routine is configured to validate at least one of the CMOS memory and the NVRAM; wherein the second validation routine is configured to validate at least one of the CMOS memory and the NVRAM **[i.e., referring to Figures 2 and 3, in block 308, the current program in flash memory 108 is for verifying and/or validating the source and content of the flash memory upgrade program, in which the "the first validation routine is configured to validate at least one of the CMOS memory and the NVRAM and the second validation routine is configured to validate at least one of the CMOS memory and the NVRAM" is considered to be part of the flash memory upgrade program routine (column 9 lines 38-40)]**.

     m.   *Referring to claim 28:*

      i.   Mattison further teaches:

         (1)   comprising a processing system operatively coupled to the first section of non-volatile memory and to the second section of non-volatile memory **[i.e., referring to Figure 2, a system memory controller is included which provides a mode where the processor is restricted to accessing only the flash**

memory, which includes "**the first section of non-volatile memory and to the second section of non-volatile memory**" (i.e., a mode where the processor can only execute instructions from the flash memory and not from any other memory such as a main system memory or cache) (column 2, lines 58-63)].

n.   *Referring to claims 29 and 42:*

i.   These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

o.   *Referring to claims 30, 36, 43, and 49:*

i.   These claims have limitations that is similar to those of claims 7-10, thus they are rejected with the same rationale applied against claims 7-10 above.

p.   *Referring to claims 31-35, 37-41, 44-48, and 50-54:*

i.   These claims have limitations that is similar to those of claims 11-15, thus they are rejected with the same rationale applied against claims 11-15 above.

q.   *Referring to claim 55:*

i.   Mattison further teaches:

(1)   performing at least one of a self-correcting, reset, and default function if the first hash does not match the second hash [**i.e., the BIOS first performs a Power On Self Test (POST), in which all the system hardware units (such as the interrupt controller, the Direct Memory Access (DMA) controller, and timers/counters) are tested and programmed for normal operation, wherein "a self-correcting, reset, and default function if the first hash does not match the second hash" is considered to perform using this same Power On Self Test (POST) (column 1, lines 16-20)**].

4.   Claims 11, 20, 31, 37, 44, and 50 are alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (US 5, 778, 070) and Miller (US 6,308,265 B1), and further in view of Davis et al (US 6, 401, 208 B2).

a.   *Referring to claims 11, 20, 31, 37, 44, and 50:*

      i.   Assuming *arguendo* that Mattison and Miller do not really point out:

      (1)   wherein the boot-block program does not allow the system to boot if the first hash does not match the second hash, and wherein the boot block program does allow the system to boot if the first hash matches the second hash;

      ii.   Davis, however, teaches:

      (1)   Concurrent or subsequent to this data transfer, within the cryptographic device, the BIOS certificate is decrypted using the root certification key (block 660). This operation is performed to retrieve a public key of the signatory of the BIOS signature (e.g., BIOS vendor). Then, the preloaded digest signature is decrypted using the public key of the BIOS vendor, for example, to recover a pre-loaded digest (block 665). After recovering the pre-loaded digest, the BIOS code is read and undergoes the one-way hash function to produce a resultant digest (block 670). The resultant digest is compared to the pre-loaded digest (block 675). If no match occurs, the host processor is precluded from continuing its boot procedure (blocks 680 and 685). However, if there is a match, the BIOS code has been authenticated as valid, which permits the host processor to execute the software code, that means continuing its boot procedure **(column 5, lines 66-67 through column 6, lines 1-13).**

      iii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

      (1)   utilize the booting procedure of Mattison with the cryptographic device to authenticate software code, loaded into the cryptographic device during a boot procedure, before permitting the host processor to execute the software code **(column 1, lines 64-67 of Davis).**

      iv.   The ordinary skilled person would have been motivated to:

      (1)   utilize the booting procedure of Mattison with the cryptographic device for the necessity in providing a protected environment for execution of code and for manipulation of data within a computer **(column 1, lines 58-60 of Davis).**

Response to Argument

5.   Applicant's arguments filed on March 25, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

When prior art references require a selected combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention itself, i.e., something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination.

Examiner totally disagrees with the applicant and still maintains that:

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Furthermore, Miller also teaches the boot block code will perform a check sum or other validation procedure on the BIOS code to determine whether the BIOS code is operable. If it is operable, then the boot block code provides a jump to the BIOS code. If the BIOS code is inoperable (e.g., check sum failed), then the boot block code will execute a recovery process to force the user to write in a new BIOS image, which is flashed into the EPROM. The boot block code typically goes into a recovery mode for any of the following reasons: a) the check of the BIOS image (e.g., check sum) reveals that the BIOS image is faulty, b) a jumper is placed (by the user) such that the recovery process is initiated, or c) a jumper plug is placed in the parallel port of the PC, again causing the recovery process to be initiated (column 4, lines 58-67 through column 5, lines 1-5 of Miller). Besides, Mattison and Miller do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably

distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of Mattison and Miller and the combination of Mattison, Miller, and Davis are sufficient.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

6.   Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

June 6, 2005

KIM VU

SUPERVISORY PATENT EXAM

TECHNOLOGY CENTER